Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1.-18. (Canceled).

19. (Currently amended) A computer system, comprising:

a computer component;

a biometric sensor;

a control unit coupled to said biometric sensor;

a lock coupled to and controlled by said control unit, wherein the control unit operates the lock by authenticating biometric data received from the biometric sensor; and

a registry stored in a memory accessible by said control unit, said registry including a first access code and a second access code,

wherein the lock prevents the computer component from being removed from the computer system unless the control unit authenticates biometric data received from the biometric sensor and obtains the first access code from the registry;

wherein logical access to the computer component is prevented unless the control unit authenticates biometric data received from the biometric sensor and obtains the second access code;

wherein the first access code enables physical access to the computer component, but not logical access; and

wherein the second access code enables logical access to the computer component, but not physical access.

20. (Previously presented) The computer system of claim 19 wherein the biometric sensor comprises a fingerprint scanner.

21. (Previously presented) The computer system of claim 19 wherein the biometric sensor comprises an iris scanner.

22. (Previously presented) The computer system of claim 19 wherein the lock comprises an electromechanical lock.

23. (Canceled).

24. (Previously presented) The computer system of claim 19 wherein said control unit verifies the authenticity of a person that has activated one of the plurality of biometric sensors based on biometric templates stored in said registry.

25. (Previously presented) The computer system of claim 24 wherein said control unit unlocks the lock if said control unit successfully verifies biometric data of a first person and wherein said control unit grants logical access to the computer component if said control unit successfully verifies biometric data of a second person.

26. (Previously presented) The computer system of claim 19 wherein said control unit maintains the lock in a locked state if said control unit cannot verify the authenticity of a person.

27. (Previously presented) The computer system of claim 19 further comprising a plurality of biometric sensors and a plurality of computer components wherein each of said plurality of biometric sensors is associated with a corresponding one of said plurality of computer components.

28. (Previously presented) A security method for a computer system including a plurality of computer components, comprising:

registering a first user's biometric to access a computing component logically;

registering a second user's biometric to access the computer component physically;

authenticating a user identity using biometrics;

if the user identity is authenticated as the first user, permitting logical access to the computer component, but not physical access; and

if the user identity is authenticated as the second user, permitting physical access to the computer component, but not logical access.

29. (Previously presented) The method of claim 28 wherein authenticating a user identity using biometrics comprises using a fingerprint sensor.

30. (Previously presented) The method of claim 28 wherein authenticating a user identity using biometrics comprises using a iris scanner.

31. (Previously presented) The method of claim 28 wherein at least one of said computer components comprises a storage device.

32. (Previously presented) The method of claim 28 wherein at least one of said computer components comprises a storage device and wherein permitting logical access to the computer component comprises permitting a user to read data from but not write data to said storage device.

33. (Previously presented) The method of claim 28 wherein at least one of said computer components comprises a storage device and wherein permitting logical access to the computer component comprises permitting a user to write data to but not read data from said storage device.

34. (Previously presented) The method of claim 28 wherein at least one of said computer components comprises a storage device and wherein permitting logical access to the computer component comprises permitting a user to read data from and write data to said storage device.

35. (Previously presented) The method of claim 28 wherein at least one of said computer components comprises a CD ROM.

36. (Previously presented) The method of claim 28 wherein at least one of said computer components comprises a hard disk drive.

37. (Previously presented) The method of claim 28 wherein said authenticating a user identity using biometrics is performed when a software program needs to access one of said computer components.

38. (Previously presented) The method of claim 37 wherein at least one of said computer components comprises a storage device.

39. (Canceled).

40. (Previously presented) The method of claim 28 further comprising acquiring a user's biometric image and associating a security access code with said biometric image.

41. (Currently amended) A biometric access system for a computer system that includes a plurality of computer devices, comprising:

a plurality of biometric sensors; and

a control unit coupled to said plurality of biometric sensors, said control unit selectively controlling logical access and physical access to the plurality of computer devices in said computer system based on signals from one or more of said biometric sensors;

wherein the control unit selectively enables a first user to have logical access to at least one of the computer devices, but not physical access;

wherein the control unit selectively enables a second user to have physical access to at least one of the computer devices, but not logical access.

42. (Previously presented) The biometric access system of claim 41 wherein at least one of said plurality of biometric sensors comprises a fingerprint scanner.

43. (Previously presented) The biometric access system of claim 41 wherein at least one of said biometric sensors comprises an iris scanner.

44. (Previously presented) The biometric access system of claim 41 wherein said control unit permits a person to access one of said plurality of computer devices based on a signal from the biometric sensor associated with the computer device that the person is trying to access.

45. (Previously presented) The biometric access system of claim 41 wherein said control unit prevents a person from accessing one of said plurality of computer devices based on a signal from its associated biometric sensor.

46. (Original) The biometric access system of claim 41 further including a registry accessible by said control unit, said registry including biometric templates of people that are permitted use of various of said computer devices.

47. (Original) The biometric access system of claim 46 wherein said control unit verifies the authenticity of a person that has activated a biometric sensor by using the templates stored in said registry.

48. (Previously presented) The biometric access system of claim 47 wherein said control unit permits a user to use one of said plurality of computer devices if said control unit successfully verifies the authenticity of a person.

49. (Previously presented) The biometric access system of claim 48 wherein at least one of said plurality of computer devices comprises a storage device.

50. (Previously presented) The biometric access system of claim 47 wherein said control unit prevents a user from using one of said plurality of computer devices if said control unit cannot verify the authenticity of the person.

51. (Previously presented) The biometric access system of claim 41 wherein at least one of the computer devices comprises a storage device.

52.-63. (Canceled).

64. (Currently amended) A security system for a server rack, said security system comprising:
a biometric sensor;
a control unit coupled to said biometric sensor; and
a lock coupled to and controlled by said control unit;
wherein the control unit selectively controls the lock to allow physical removal of a server based on data received from the biometric sensor,
wherein the control unit selectively controls logical access to the server based on data received from the biometric sensor,
wherein the control unit selectively enables a first user to have logical access to the server, but not physical access;
wherein the control unit selectively enables a second user to have physical access to the server, but not logical access.

65. (Previously presented) A security system as defined in claim 64, wherein the biometric sensor is located remotely from the server rack.

66. (Previously presented) A security system as defined in claim 64, further comprising:

a rack for holding a plurality of servers.

67. (Previously presented) A security system as defined in claim 66, further comprising a plurality of locks to secure each of a plurality of servers to the rack.

68. (Canceled).

69. (Previously presented) A security system as defined in claim 64, further including a registry stored in memory accessible by said control unit, said registry including a template for each person authorized to unlock the lock.

70. (Previously presented) A security system as defined in claim 69, wherein said control unit verifies the authenticity of a person that has activated the biometric sensor by using the templates stored in said registry.

71. (Previously presented) A security system as defined in claim 64, wherein the biometric sensor is selected from among a fingerprint sensor and an iris scanner.

SUBSTANCE OF THE INTERVIEW STATEMENT

Mr. Christenson and Examiner Brown discussed the claims on August 15, 2006. The language of allowable claim 28 was reviewed and compared to other claims. Mr. Christenson inquired whether claim amendments could be entered after the final rejection to place the rejected claims in allowable form. Examiner Brown generally agreed to consider entering claim amendments after the final rejection. To facilitate entry of the claim amendments and allowance of the amended claims, Applicant has amended claims 19, 41 and 64 to incorporate features similar to the allowable subject matter indicated by the Examiner in the reasons for allowance of claim 28.